D.DATA PRIVACY IN CYBERSPACE

The term 'right to privacy' could be taken to mean an individual's right to be free from intrusion or interference by others. Cyber space means a non-physical terrain created by computers. Most often than not, in the recent times, citizens (also referred to as 'netizens') have been increasingly making use of the cyber space to seclude themselves from their social circle. There is a general belief that these people are private and want to secure their privacy. In reality, it turns out that there is a serious threat of infringement of privacy of an individual in the cyber space. In order to recognize digital evidence and electronic records in India, the Information Technology Act came into force on and from 2000.

The cybercrime is an evolving field and therefore with changing times, more and more crimes that emerge from violations committed in the cyber space is detected. The common forms of the cybercrimes have been broadly categorized into those against person and against property.

The categories of the crimes against persons in the cyber space could include:

- Harassment via E-Mails: The said offence is one wherein the sender tries to harass the victim by sending emails, text, messages, pictures, videos, attachments and folders by way of harassing the victim.
- Cracking: This offence is committed when the computer system of an individual is compromised without the knowledge of the victim and the confidential data is accessed without consent and is tampered.
- Cyber-Stalking: This is a form of harassment, when the offender constantly harasses the victim through electronic means. The electronic means would include internet, e-mail, phones, text messages, webcam, websites or videos.
- Hacking: This is the most common form of crime that is known to the users of the cyber space. Hacking basically means taking complete control and access over the computer system and destroying the entire data that is available. Hacking could also be done over the telecommunication and mobile network.
- Dissemination of Obscene Material: This refers to the offence, whereby the offender exhibits material relating to indecent exposure or pornographic content or hosting prohibited content.
- Spoofing: This basically refers to stealing of identity of a person. By stealing the identity of the victim, the offender will make use of the identity of the victim to communicate to third persons. It would appear as though the victim is indulging in such communication.
- Page jacking: This is an offence, wherein the website of a victim is compromised and is used to link some other fake website. In effect, when a user clicks on the link of the website of the victim, he would be linked to the fake site. Thus, the search engines can be tricked to list the fake website.
- Carding: The electronic magnetic field of the ATM cards including credit cards are stolen and are used by the offender to swipe off the money from the victim's account.
- Other crimes: Any other crime like cheating, fraud, threat to life and other forms of crime punishable under the Indian Penal Code, when committed with the help of the electronic devices or by making use of the cyber space, it falls within the ambit of cybercrime against persons.

It is to be noted however, that every act of infringement of privacy is not made a cybercrime. Therefore, irrespective of the above offences, there is need for awareness with respect to the privacy rights of an individual that is infringed in the cyber space. They are:

- Spamming: Though the browsing history is not saved, often the users are perplexed when the internet service provider and the other websites visited send out a whole-lot of unwarranted messages by tracking the websites visited by them (both through ordinary browsing and through incognito web browsing). This is called spamming and usually the browser in not aware as to why the messages were sent to him. Therefore, what is required is awareness with regard to the effects of using the cyber space.
- Unauthorized Access: Likewise, during chats and other conversations over the internet, persons share their personal details, which could be used by the tracking system. It is also important to note that the information the user shares over the internet could be accessed by large number of people. This is especially crucial in the case of social networking sites where people share their personal information. Any unauthorized access to the personal information or misuse of information is likely to affect a person's right to privacy in a serious manner.

The Telecom Commercial Communications Customer Preference Regulations 2010 is one of the pieces of regulations, which prevents the service providers from arbitrary sharing of personal information. Access Providers as defined under the regulations include the Basic Telephone Service Provider, Cellular Mobile Telephone Service Provider and Unified Access Service Provider. Thus, all forms of service providers are included within the regulations and the licence holders have to act in accordance with the regulations prescribed therein. Thus, all the service providers have to take necessary measures to protect the privacy and information shared on their networks.

To conclude, it is found that each individual accessing the cyber space ought to be better informed about the advantages and disadvantages of using the same. It is necessary to be a responsible user of the cyber space and awareness is the key. The law in respect to the right to privacy with respect to cyber space is still in its nascent stage and therefore, the individuals have a key role to ensure that their rights to privacy are not intruded due to ignorance.